

Notice of Allowability

Application No.

09/940,985

Examiner

Zachary A. Davis

Applicant(s)

KAMINAGA ET AL.

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the RCE and submission dated 17 March 2007 and supplemental reply dated 12 April 2007.

2. ☒ The allowed claim(s) is/are 5-10.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☒ All b) ☐ Some* c) ☐ None of the:

1. ☒ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____

7. ☐ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____


EMMANUELLE L. MOISE
SUPERVISORY PATENT EXAMINER

Notice of Allowability	Application No.	Applicant(s)	
	09/940,985	KAMINAGA ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the RCE and submission dated 17 March 2007 and supplemental reply dated 12 April 2007.

2. ☒ The allowed claim(s) is/are 5-10.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☒ All b) ☐ Some* c) ☐ None of the:

1. ☒ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____

7. ☐ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____


EMMANUELLE L. MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Per Applicant's instructions (see page 5 of the submission received 19 March 2007), the amendment received 19 January 2007 has NOT been entered. Applicant's submission filed on 19 March 2007 has been entered.
2. By the above submission, Claims 5-7 have been amended. Claims 11-13 have been canceled. No new claims have been added. Claims 5-10 are currently pending in the present application.

Response to Amendment

3. The supplemental reply received 12 April 2007 was not filed during a period of suspension of action as set forth in 37 CFR 1.111(a)(2)(ii) and thus its entry is not a matter of right. However, because the reply is clearly limited to adoption of the

Art Unit: 2137

Examiner's suggestions, as provided for by 37 CFR 1.111(a)(2)(i)(B), the reply has been entered.

4. By the above supplemental reply, Claims 5 and 6 have been further amended. Claims 5-10 remain pending in the present application.

Allowable Subject Matter

5. Claims 5-10 are allowed.
6. Reasons for allowance were set forth in the Office action mailed 01 May 2006.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
 - a. Folmsbee, US Patent 6308256, discloses a system in which instructions are obfuscated by varying the sequence in which registers are read from.
 - b. McGrath et al, US Patent 6438664, discloses a system in which register read and write operations can be performed out of order.
 - c. Lin et al, UK Patent Application GB 2345229, discloses an encryption system that resists differential power analysis attacks by varying the order in which blocks are combined.

Art Unit: 2137

d. Velten et al, German Patent Document DE 19845073, discloses a method for preventing differential power analysis by randomly varying the order of evaluation of substitution boxes in an encryption algorithm.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 09/940,985

Page 5

Art Unit: 2137

240
zad


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER